LISTING OF CLAIMS

1. (**Currently Amended**) A security protocol method comprising:

cryptographically hashing a platform configuration value from a platform configuration register (PCR) in a trusted platform module (TPM) that indicates integrity of an endpoint platform, the platform configuration value representing a configuration state of the endpoint platform that indicates an integrity of the endpoint platform to generate a cryptographic hash of the platform configuration;

~~**mixing, via a hash algorithm to generate**~~ **generating** a master ~~**secret,**~~ **secret by hashing together** the cryptographic hash of the platform configuration with a pre-master secret **from which the master secret is derived,** and data from a stored measurement log that stores configuration state measured values for the endpoint platform;

negotiating a communication channel;

signing the **generated** master secret with multiple authentication facets of the endpoint, the multiple authentication facets including a user key representing a particular user and a platform key representing the particular endpoint platform **to produce a master secret signed with multiple authentication keys to authenticate the endpoint**;

authenticating**, as part of a bidirectional handshaking protocol exchange,** the negotiated communication channel with the signed master secret to establish the negotiated communication channel as a secure channel to achieve late binding of the secure channel **to prevent the binding from persisting outside the secure channel**, including generating a session key for the communication channel, where the session key is generated from the master secret.

2. (Previously Presented) The method of claim 1, wherein a platform private key is bound to the platform configuration using the TPM.

3. (Previously Presented) The method of claim 2, wherein the TPM comprises a processor coupled to a protected storage device.

4. (Original) The method of claim 1, wherein cryptographically hashing the platform configuration comprises cryptographically hashing the platform configuration using a secure hashing algorithm.

5. (Original) The method of claim 4, wherein the secure hashing algorithm comprises Secure Hashing Algorithm Version 1.0 (SHA-1).

6-9. (Canceled)

10. (Previously Presented) The method of claim 1, wherein the platform configuration includes multiple identities and the platform key includes one or more platform identity keys.

11. (Previously Presented) The method of claim 1, wherein the platform configuration includes multiple identities and the platform key includes each platform configuration identity key.

12. (Canceled)

13. (Original) The method of claim 1, further comprising:

exchanging an explanation of the platform configuration hashes following session key negotiations to finalize the authentication;

verifying, at both endpoints, key exchange messages, certificates and platform configuration data; and

authenticating the session if no problems arise during verification.

14. (Original) The method of claim 13, further comprising halting the authentication session if problems arise during verification.

15. (Original) The method of claim 13, further comprising enabling endpoints to exchange data, wherein each endpoint knows that the platform from the other endpoint has been authenticated using a platform identity that ties to the trusted platform module.

16-32. (Canceled)

33. **(Currently Amended)** ~~**An article comprising: a tangible**~~ **A computer readable** storage medium having ~~**a plurality of machine accessible**~~ instructions stored thereon, ~~**wherein**~~ **which** when ~~**the instructions are**~~ executed by a processor, ~~**the instructions**~~ provide for simultaneously authenticating multiple facets of an ~~**endpoint;**~~ **endpoint by:**

cryptographically hashing a platform configuration value from a platform configuration register (PCR) in a trusted platform module (TPM) that indicates integrity of an endpoint platform, the platform configuration value representing a configuration state of the endpoint platform that indicates an integrity of the endpoint platform to generate a cryptographic hash of the platform configuration;

~~**mixing, via a hash algorithm to generate**~~ **generating** a master ~~**secret,**~~ **secret by hashing together** the cryptographic hash of the platform configuration with a pre-master secret **from which the master secret is derived,** and data from a stored measurement log that stores configuration state measured values for the endpoint platform;

negotiating a communication channel;

signing the **generated** master secret with multiple authentication facets of the endpoint, the multiple authentication facets including a user key representing a particular user and a platform key representing the particular endpoint platform **to produce a master secret signed with multiple authentication keys to authenticate the endpoint**;

authenticating**, as part of a bidirectional handshaking protocol exchange,** the negotiated communication channel with the signed master secret to establish the negotiated communication channel as a secure channel to achieve late binding of the secure channel **to prevent the binding from persisting outside the secure channel**, including generating a session key for the communication channel, where the session key is generated from the master secret.

34. (Previously Presented) The article of claim 33, wherein a platform private key is bound to the platform configuration using the TPM.

35. (Previously Presented) The article of claim 34, wherein the TPM comprises a processor coupled to a protected storage device.

36. (Original) The article of claim 33, wherein instructions for cryptographically hashing the platform configuration comprises instructions for cryptographically hashing the platform configuration using a secure hashing algorithm.

37. (Original) The article of claim 36, wherein the secure hashing algorithm comprises Secure Hashing Algorithm Version 1.0 (SHA-1).

38-41. (Canceled)

42. (Previously Presented) The article of claim 33, wherein the platform configuration includes multiple identities and the platform key includes one or more platform identity keys.

43. (Previously Presented) The article of claim 33, wherein the platform configuration includes multiple identities and the platform key includes one or more platform identity keys.

44. (Canceled)

45. (Original) The article of claim 33, further comprising instructions for:

exchanging an explanation of the platform configuration hashes following session key negotiations to finalize the authentication;

verifying, at both endpoints, key exchange messages, certificates and platform configuration data; and

authenticating the session if no problems arise during verification.

46. (Original) The article of claim 45, further comprising instructions for halting the authentication session if problems arise during verification.

47. (Original) The article of claim 45, further comprising instructions for enabling endpoints to exchange data, wherein each endpoint knows that the platform from the other endpoint has been authenticated using a platform identity that ties to the trusted platform module.